

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 01-101042

(43)Date of publication of application : 19.04.1989

(51)Int.Cl.

H04L 9/00

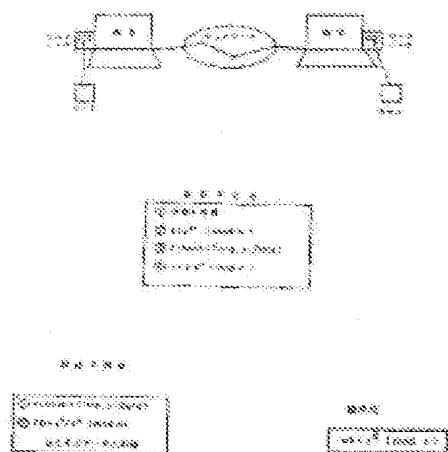
(21)Application number : 62-259023

(71)Applicant : NEC CORP

(22)Date of filing : 13.10.1987

(72)Inventor : OKAMOTO EIJI

(54) AUTHENTICATION DEVICE



(57)Abstract:

PURPOSE: To prevent a dishonest resending by a third party by preparing integers dependent of a time and an authenticator and providing a deciding means to decide whether the identification information of a sending side is made or not.

CONSTITUTION: To each user, a card, onto which integers (n), α , e1 and S_i of the degree of 512 bits are written, is distributed from a card publisher or a center. Only the S_i is the secret integer different for each user, and the others are common to each user. In forming an authenticator, a random number (r) is generated, and $x = \alpha \cdot r \pmod{n}$ is calculated from (e), α and (n) read out of the card of the user. Next, the hash function value of data Data to be transmitted, a time Time and an above-mentioned integer (x), $C = \text{hash}(\text{Time}, x, \text{Data})$ is calculated. Next, whether a sent authenticator (x, y) and

$Y = x \cdot C \pmod{n}$ such as the (e), (n) and (x) from the card of the receiving side user are equal to an ID information ID1 of the transmitting side user or not is decided.

⑫ 公開特許公報(A)

平1-101042

⑤Int.Cl.⁴

H 04 L 9/00

識別記号

庁内整理番号

A-7240-5K

④公開 平成1年(1989)4月19日

審査請求 未請求 発明の数 3 (全4頁)

⑬発明の名称 認証装置

⑭特 願 昭62-259023

⑮出 願 昭62(1987)10月13日

⑯発 明 者 岡 本 栄 司 東京都港区芝5丁目33番1号 日本電気株式会社内

⑰出 願 人 日本電気株式会社 東京都港区芝5丁目33番1号

⑱代 理 人 弁理士 内 原 晋

明 細 書

発 明 の 名 称 認証装置

特 許 請 求 の 範 囲

1. 認証子を作成する認証装置において、ランダムな整数 r を生成する乱数生成手段と、あらかじめ定められた複数の整数を記憶する記憶手段と、少なくとも時刻と前記乱数とに依存した整数 c を生成するハッシュ化手段と、前記の複数の整数と c 、 r から認証子を生成する認証子生成手段と、から成ることを特徴とする認証装置。

2. あらかじめ定められた複数の整数とランダムに選んだ整数 r と少なくとも時刻と該乱数に依存した整数 c から作成した認証子を送り側から受取り、認証を行なう認証装置において、少なくとも時刻と前記認証子に依存した整数 c_1 を生成するハッシュ化手段と、前もって定められた複数の整数を記憶する記憶手段と、該整数と認証子と c_1 からあらかじめ定められた変換を施した結果が送

り側の識別情報になっているか否かを判定する判定手段と、から成ることを特徴とする認証装置。

3. 通信相手に送るべき認証子を作成し、鍵を作成する認証装置において、ランダムな整数 r を生成する乱数手段と、あらかじめ定められた複数の整数を記憶する記憶手段と、少なくとも時刻と前記乱数とに依存した整数 c を生成するハッシュ化手段と、前記複数の整数と c 、 r から認証子を生成する認証子生成手段と、通信相手から送られた認証子が正しければそれと前記 r を用いて鍵を生成する鍵生成手段と、から成ることを特徴とする認証装置。

発 明 の 詳 細 な 説 明

(産業上の利用分野)

本発明はネットワークにおいて、通信相手ユーザあるいはメッセージの認証さらには通信の略号化に関する。

(従来技術)

認証方式として

エー・シャミア(A. Shamir)がクリプト84(Crypt

0.04)で提案した方式は、各ユーザの氏名などのID情報を用いた実用的方式として評価が高い。
(発明が解決しようとする問題点)

シャミアの方式には次の2つの欠点がある。

1つは、正当なユーザから別の正当なユーザへの送信文を第三者が録音しておき、後にそれを再生送信すると受信者がその不正を検出できないことである。さらにもう1つは暗号通信と組合せようとすると、その鍵を送るための情報帯域が新たに必要となる。

(問題点を解決するための手段)

本発明によれば、認証子を作成する認証装置において、ランダムな整数 r を生成する乱数生成手段と、あらかじめ定められた4つの整数 n 、 α 、 e 、 s を記憶する記憶手段と、少なくとも時刻と前記乱数とに依存した整数 c を生成するハッシュ化手段と、前記の整数 n 、 α 、 e 、 s 、 c 、 r から2つの整数 $\alpha^{e \cdot r}(\text{mod } n)$ と $S \cdot \alpha^{c \cdot r}(\text{mod } n)$ から成る認証子を作成する認証子生成手段と、から成ることを特徴とする認証装置が得られる。

れた認証子が正しければそれと前記整数 r を用いて鍵を生成する鍵手段とから成ることを特徴とする認証装置が得られる。

(作用)

第1図は本発明の作用・原理を示すごく大まかな流れ図である。以下、認証子を作成する側を証明側、認証子を検証する側を認証側とよぶことにする。証明側は、認証側が検証を行えるような認証子を作成して他の必要なデータと共に送る。これが第1図(a)である。一方、認証側では送られた認証子の正否を判断する。これが第1図(b)である。さらに、受信側では暗号用の鍵を該認証子を用いて秘密に作成することができ、これが第1図(c)である。暗号通信の相手側も同じ暗号用の鍵を持たなくてはならないが、これは受信側が(a)の証明側となって認証子を送信側に送り、該送信側が認証側となって(c)を実行すればよい。

(実施例)

第2図は本発明の一実施例を示す構成図である。ネットワークを介して接続されている端末の

また、本発明によれば、あらかじめ定められた4つの整数 n 、 α 、 e 、 s とランダムに選んだ整数 r と少なくとも時刻に依存した整数 c から作成した2つの整数 $\alpha^{e \cdot r}(\text{mod } n)$ と $S \cdot \alpha^{c \cdot r}(\text{mod } n)$ から成る認証子 (x, y) を送り側から受取り、認証を行なう認証装置において、少なくとも時刻と前記認証子に依存した整数 c_1 を生成するハッシュ手段と、前記整数 n と e を記憶する記憶手段と、前記整数 n 、 e 、 x 、 y 、 c_1 に対して $y \cdot x^{c_1}(\text{mod } n)$ が送り側の識別情報になっているか否かを判定する判定手段と、から成ることを特徴とする認証装置が得られる。

さらに本発明によれば、通信相手に送るべき認証子を作成し、鍵を生成する認証装置において、ランダムな整数 r を生成する乱数生成手段と、あらかじめ定められた4つの整数 n 、 α 、 e 、 s を記憶する記憶手段と、少なくとも時刻と前記乱数に依存した整数 c を生成するハッシュ化手段と、前記の整数 n 、 α 、 e 、 s 、 c 、 r から2つの整数 $\alpha^{e \cdot r}(\text{mod } n)$ と $S \cdot \alpha^{c \cdot r}(\text{mod } n)$ から成る認証子を作成する認証子生成手段と、通信相手から送ら

1つを送信ユーザが利用し、別の1つを受信ユーザが利用するものとする。各端末にはカードリーダーが設置され、端末には認証のためのソフトあるいはハードが組込まれ、第1図を実行する。各ユーザには512ビット程度の整数 n 、 α 、 e 、 S_i が書込まれたカードがカード発行者(又はセンター)から配布される。ここで S_i のみがユーザ毎に異なる秘密の整数で他は各ユーザに共通である。ユーザ i のID情報を ID_i とすると、 S_i は

$$S_i = (ID_i \cdot \alpha^{e \cdot r}(\text{mod } n)) \cdot \alpha^{c \cdot r}(\text{mod } n)$$

を満たすように作られている。このようにできることは、コミュニケーション・オブ・ザ・エーシーエム(Communication of the ACM)第21巻 2号120頁～126頁に示されている。

端末がなすべき作業は第1図に示してあるが、その中の認証子作成、認証子検証、鍵生成の実施例を各々第3、4、5図に示す。

認証子作成では乱数 r を生成し、ユーザのカー

ドから読出した e 、 α 、 n から $x = \alpha^{e \cdot r} \pmod{n}$ を計算する。次々に送るべきデータ $Data$ と時刻 $Time$ と前記整数 x のハッシュ関数値、 $C = hash(Time, x, Data)$ を計算する。ここでハッシュ関数 $hash$ は例えばアイイーイーイー(IEEE)の確認コンピュータ(COMPUTER)誌1983年2月号55頁～62頁に記載されている関数である。 $Data$ は謂ゆるメッセージ以外にも送信者のID情報やその他のデータを含めてもよい。このとき、認証子 (x, y) は上記 x と

$$y = Si \cdot d^{e \cdot r} \pmod{n}$$

で与えられる。 Si もユーザのカードから読み出した整数である。

第4図の認証子検証では前記ハッシュ関数により同様に $c = hash(Time, x, Data)$ を計算する。ここで $Data$ は送信側から送られたデータであり、 $Time$ は送信側が認証子作成の際に用いた時刻情報であり、受信側で正しくわからない場合には $Time$ を送ってもらう必要がある。 x は送られた認証子の一部である。次に送られて認証子 (x, y) と受信側ユーザのカードからの

e 、 n 、 x 、 r

$$y^e / x^e \pmod{n}$$

が送信側ユーザのID情報 ID_i に等しいか否かを判定する。もし等しくなければ不正データとみなす。送信側ユーザが送った (x, y) を用いれば、 x, y の定義から、 n を法として

$$y^e / x^e = Si^e \cdot \alpha^{e \cdot r \cdot e} / \alpha^{e \cdot r \cdot e} = ID_i$$

となる。

第5図の鍵生成では、乱数 R を用いて、

$$WK = X^R \pmod{n}$$

により作成する。ここで x は認証側から送られたものであり、乱数 R は認証子作成に用いた乱数である。即ち、受信側でも鍵生成の場合には(作用)の項で述べたように認証子作成を行なうが、その時に用いた乱数 R である。送信側でも認証子作成に用いた乱数 r を鍵生成に用いる。いずれの側でも WK は $\alpha^{e \cdot r \cdot R} \pmod{n}$ に等しくなる。

以上の実施例において、巾乗剰除 $z = a^b \pmod{n}$ の計算は端末のソフトで行なうことも、プロ

セッサで行なうこともできる。また、時刻情報 $Time$ は時刻そのものではなく、毎回異なるようなビットパターンでもよく、時刻により変わるものならよい。

(発明の効果)

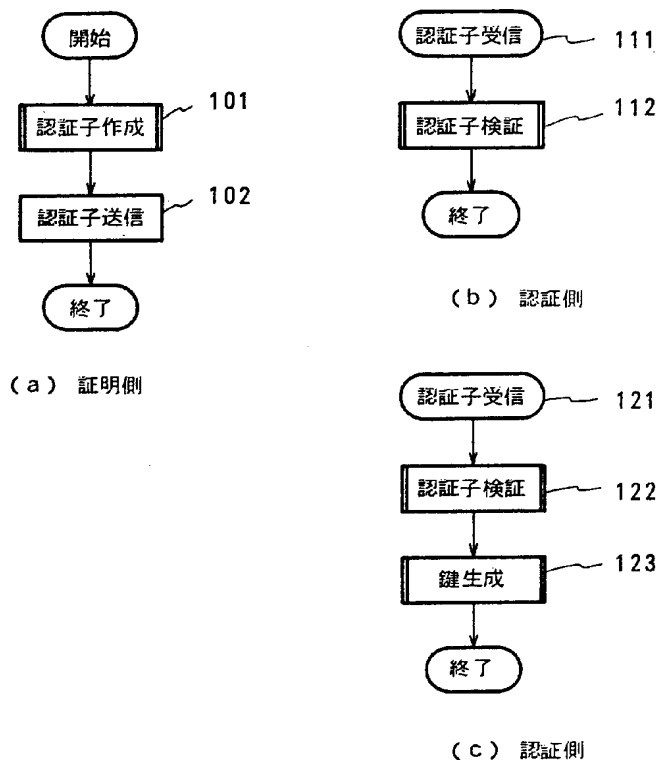
以上、詳細に説明したように、本発明を用いれば第三者による不正再送を防ぎ、あるいは暗号用の鍵生成も行なえるという機能付きの認証が実行できるのでネットワーク通信などに有用である。

図面の簡単な説明

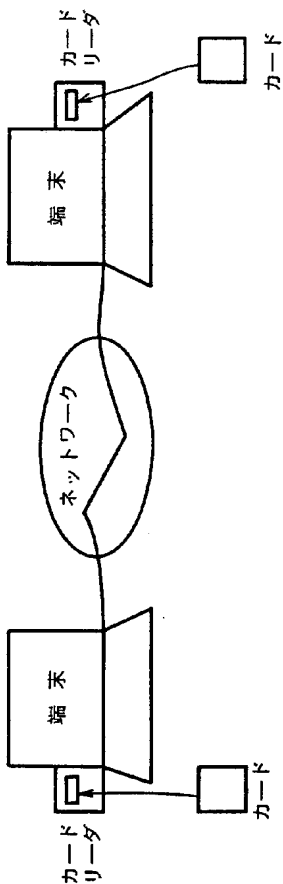
第1図は本発明の作用・原理を示す流れ図、第2図は本発明の実施例を示す構成図、第3、4、5図は第1図の認証子作成、認証子検証、鍵生成の各実施例を示す図である。図において、101は認証子作成機能、102は認証子送信機能を、111、121は認証子受信状態を、112、122は認証子検証機能を、123は鍵生成機能を各々を示す。

代理人 弁理士 内原 晋

第 1 図



第 2 図



第 4 図

認証子検証

① $c = \text{hash}(\text{Time}, x, \text{Data})$
② $ID * y^c / x^c \pmod n$
なら不正データと判断

第 3 図

認証子生成

① 乱数 r 生成
② $x = a^{*r} \pmod n$
③ $c = \text{hash}(\text{Time}, x, \text{Data})$
④ $y = s \cdot a^{*cr} \pmod n$

第 5 図

鍵生成

$wk = x^R \pmod n$